시각암호의 휘도 개선을 위한 새로운 구성법

양신석[†] · 김문수[††] · 박지환[†††]

요 약

시각암호는 복잡한 암호학적 연산 없이 인간의 시각에 의해 비밀정보를 직접 복원할 수 있는 간단한 방식이다. 이 방식은 영상 형태의 비밀정보를 n개의 랜덤한 영상(슬라이드)으로 분산시킬 때, 각 화소가 확장되면서 복원영상의 크기가 커지고 휘도가 떨어지는 결점이 있다. 따라서, 확장 화소의 수를 줄이고 휘도를 개선하는 연구가 많이 이루어 져 오고 있다. 본 논문에서는 기저행렬의 행을 중첩시켜 (k, n) 시각암호의 휘도를 개선하기 위한 새로운 구성법을 제안하고, 그룹 내 n개의 슬라이드 중 k개 이상의 슬라이드를 선택하는 방법에 따라 복수의 휘도를 갖는 (k, n) 시각암호를 구성할 수 있음을 보인다.

New Construction Scheme for Improving Contrast in Visual Cryptography

Sin-Sok Yang[†], Moon-Soo Kim[††] and Ji-Hwan Park[†††]

ABSTRACT

Visual cryptography is a simple method in which secret information can be directly decoded in human visual system without any cryptographic computations. This scheme is a kind of secret sharing scheme in which secret of image type is distributed to n random image(we call it share). When the secret image is distributed to n shares, the original pixel is expanded as much as the size of column in basis matrix. It causes the deterioration of contrast in decoded secret image. Therefore, many researches have performed to reduce the size of pixel expansion and to improve the contrast in decoded image. In this paper, we propose a new construction scheme to improve the contrast by overlapping the row in basis matrix for (k, n) visual cryptography. In addition, we show that the proposed method can construct the (k, n) visual cryptography with multiple contrasts depending on selecting k out of n slides in a group.

1. 서 론

기밀정보에 대한 보안을 유지하기 위해서 그 정보를 여러 개로 분산시켜 임의의 문턱치(threshold)를 만족하면 그 비밀에 대한 정보를 복원할 수 있고, 그렇지 않으면 기밀 정보에 대한 어떠한 내용도 알 수 없도록 하는 비밀 분산법이 A. Shamir에 의하여 제안되었다[1]. 이 비밀 분산법은 암호화 및 복호를 위한 연산량이 많고 구성이 복잡한 문제점이 있다. 따라서 복잡한 암호학적 연산이 없이 인간의 시각만으로 간단히 복원할 수 있는 시각암호가 M. Naor와 A. Shamir에 의해 제안되었다[2]. (k, n) 시각암호 방식(VCS : Visual Cryptography Scheme)은 영상 형태의 비밀을 n개의 슬라이드 형태의 share로 인쇄한 후, n명에게 배포하여 k장 이상의 서로 다른 슬라이드를 중첩해야만 비밀정보를 복원할 수 있도록 한 것이다. 시각암호에 의해 분산되는 비밀영상은 흑과 백의 화소로 구성되어 슬라이드와 같이 물리적 중첩이 가능한 곳에 인쇄되는 것으로 가정한다.

원 영상의 각 화소는 n개의 share로 분산되고, 각 share는 m개의 부 화소(sub-pixel)로 확대된다. 이

본 연구는 부경대학교 1999년도 중등교원 연구비 지원에 의해 수행되었음.
† 배정고등학교 교사
†† 준회원, 부산여자고등학교 교사
††† 종신회원, 부경대학교 전자컴퓨터정보통신공학부 교수

때, m이 커지면 상대적 차(relative difference) α가 작아져서 복원영상의 시각적 인식이 어려워진다. 따라서 m을 될 수 있는 한 작게 함으로써 상대적 차 α를 높이거나[3-6], m에 의존하지 않으면서 비밀영상을 복원할 때 흑과 백화소 사이의 휘도를 높이는 방법이 요구된다.

본 논문에서는 m에 의존하지 않으면서 복원 영상의 휘도를 높이는 (k, n) 시각암호 방식의 일반적인 구성법과 여러 가지의 휘도를 허용함으로써 평균 휘도는 같지만, m의 크기를 줄일 수 있는 새로운 구성법을 제안한다. 먼저, 2장에서는 시각암호의 기본 모델과 (k, k) 시각암호를 구성하기 위한 최적의 구성법에 대하여 고찰한다. 3장에서는 (k, n) 시각암호의 새로운 구성법에 대한 구성원리를 알아보고 휘도를 분석하여 기존의 방법과 비교하며, 특수한 경우에 휘도가 개선되는 것을 보인다. 또한 (k, n) 시각암호의 구성에 있어서 개선된 휘도를 유지하면서 부 화소의 수를 줄이기 위한 새로운 접근도 제시한다. 4장에서는 m이 커지는 문제점을 개선하기 위하여 복수의 휘도를 허용하는 새로운 (k, n) 시각암호의 구성법을 제안하고, Droste방식[3]과 비교 분석하여 그 유효성을 보인다.

2. 시각암호

2.1 기본모델

시각암호에 의한 비밀분산의 가장 간단한 형태는 흑(1)과 백(0)의 화소로 구성된 이진영상(binary image)을 대상으로 하는 것이다. 비밀영상의 각 화소는 m개의 부화소로 확장되어 n장의 슬라이드에 각각 분산되며, 이것을 share라 부른다.

이 구조는 비밀영상의 각 화소를 $n \times m$ 부울 행렬 $S=[s_{ij}]$로 표현할 수 있으며, 이때 s_{ij}의 값은 i번째 share 중 j번째 부 화소가 흑일 때 1이 되고, 백인 경우는 0으로 된다. Share들을 정확하게 겹쳤을 때, 행렬 S에서 행에 대한 부울리언 "or"로 표현되는 결합share를 볼 수 있다. 결합share의 grey 레벨은 "or" 연산을 한 m차 벡터 V의 해밍 가중치 $H(V)$에 비례한다. 이 grey 레벨은 어떤 고정된 문턱치 $d(1 \le d \le m)$와 상대적 차 $\alpha > 0$에 대해서 $H(V) \ge d$이면 흑으로, $H(V) \le d - \alpha \cdot m$이면 백으로 인식된다.

[정의] (k, n) - VCS는 $n \times m$ 부울 행렬들의 두 집합 C_0, C_1으로 구성된다. 백의 화소를 분산하기 위해서 C_0의 행렬 중의 하나를 임의로 선택하고, 흑의 화소를 분산하기 위해서 C_1의 행렬 중의 하나를 임의로 선택한다. 선택된 행렬의 각 행은 한 개의 share에 대응하고 행의 각 요소가 1이면 흑을, 0이면 백을 나타낸다. 아래의 3가지 조건을 만족하면 (k, n)-VCS의 해가 유효하게 된다.

1. C_0의 임의의 행렬 S_0에 대해 n행 중 임의의 k행에 대한 "or" 연산 시 m차 벡터 V의 해밍 가중치 $H(V) \le d - \alpha \cdot m$을 만족한다.
2. C_1의 임의의 행렬 S_1에 대해 n행 중 임의의 k행에 대한 "or" 연산 시 m차 벡터 V의 해밍 가중치 $H(V) \ge d$를 만족한다.
3. $q<k$인 $\{1, 2, \cdots, n\}$의 임의의 부분집합 $\{i_1, i_2, \cdots, i_q\}$에 대해 $C_t(t \in \{0, 1\})$의 각 $n \times m$ 행렬을 $i_1, i_2, \cdots i_q$ 행으로 제한하여 얻은 $q \times m$ 행렬 $D_t(t \in \{0, 1\})$는 같은 빈도를 갖는 동일한 행렬을 포함한다.

조건 1과 2는 share를 겹쳤을 때 복원된 영상에서의 휘도(contrast)를 나타내고, 조건3은 k장미만의 share를 겹쳤을 때 분산된 화소가 흑인지 백인지를 구분할 수 없는 안전성(security)을 나타낸다.

2.2 (k, k)-VCS의 구성

(k, k)-VCS를 구성하기 위하여 k개의 원소를 갖는 전체집합 $W=\{e_1, e_2, \cdots, e_k\}$에 대하여 원소의 개수가 짝수인 부분집합의 리스트 $\pi_1, \pi_2, \cdots, \pi_{2^{k-1}}$과 원소의 개수가 홀수인 부분집합의 리스트 $\sigma_1, \sigma_2, \cdots, \sigma_{2^{k-1}}$을 고려한다.

$1 \le i \le k$와 $1 \le j \le 2^{k-1}$인 i, j에 대하여 S_0와 S_1은 $e_i \in \pi_j$일 때 $S_0[i, j]=1$, $e_i \in \sigma_j$일 때 $S_1[i, j]=1$ 로 정의되는 $k \times 2^{k-1}$ 기저행렬(basis matrix)이라 하자. S_0와 S_1의 모든 열들을 교환해서 만든 행렬의 집합을 C_0와 C_1으로 각각 나타낸다. 이 때, $m=2^{k-1}$, $\alpha=\frac{1}{2^{k-1}}$이 된다. 그림1에 (3,3)-VCS의 일 예를 나타낸다. 이 때, 부 화소의 크기 m과 상대적 차 α는 각각 4와 1/4이 된다.

$$S_0 = \begin{pmatrix} 0110 \\ 0101 \\ 0011 \end{pmatrix}, \quad S_1 = \begin{pmatrix} 1001 \\ 0101 \\ 0011 \end{pmatrix}$$
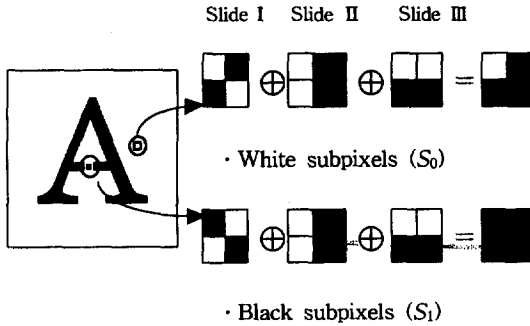
그림 1. 화소의 분산

3. (k, n)-VCS의 새로운 구성

3.1 구성원리

먼저, (k, k)-VCS에 의해 구성된 기저행렬 S_0와 S_1의 각 행에 $r_1, r_2, \cdots, r_k$의 인덱스를 차례로 부여한다. 이 때, 확장되는 부 화소의 크기는 $m_k=2^{k-1}$이고, $r_i(S_j)$ $(i\in\{1,2,\cdots,k\}, j\in\{0,1\})$는 행렬 S_j에서 r_i행을 구성하는 행 벡터를 나타낸다.

이제 각 행 $r_1, r_2, \cdots, r_k$를 각각 $p, q, \cdots, s$개씩 중복시켜 행의 개수가 n이 되는 $n\times 1$열 벡터 V를 구성한다. 단, $p+q+\cdots+s=n$과 $p\geq q\geq\cdots\geq s\geq p-1$의 조건을 만족하도록 한다. 구성되는 열 벡터 V는 다음의 형태가 된다.

$$V=\begin{pmatrix} \left.\begin{matrix} r_1 \\ \vdots \\ r_1 \end{matrix}\right\} \leftarrow p\text{개} \\ \left.\begin{matrix} r_2 \\ \vdots \\ r_2 \end{matrix}\right\} \leftarrow q\text{개} \\ \vdots \quad\quad \vdots \\ \left.\begin{matrix} r_k \\ \vdots \\ r_k \end{matrix}\right\} \leftarrow s\text{개} \end{pmatrix} = [\, r_1\cdots r_1 r_2\cdots r_2\cdots r_k\cdots r_k]^T$$

만들어진 열 벡터 V에 대하여 모든 행을 교환하여 연접한 행렬을 M이라 하면, M은 n개의 행과 ${}_nC_p\times{}_{n-p}C_q\times\cdots\times{}_sC_s$개의 열을 갖는 행렬이 되며, 확장 화소의 수

$$m=m_k\times{}_nC_p\times{}_{n-p}C_q\times\cdots\times{}_sC_s$$
$$(\text{or}\quad m=2^{k-1}\times\frac{n!}{p!\times q!\times\cdots\times s!})$$

인 $n\times m$ 기저 행렬 S_0'와 S_1'가 만들어진다.

한편, (k, n)-VCS에 대한 확장 화소의 수 m을 고려할 때 중복되는 횟수가 같은 행들은 서로 교환하여도 같은 결과를 가지게 되므로 그 행을 제거하여 m을 줄일 수 있다. 즉, 어떤 한 행에 대하여 그 행과 중복횟수가 같은 행들이 R종류 발생한다면 나머지는 $(k-R)$ 종류가 된다. 이 때, 열 벡터 V에 대한 행 교환 연접 행렬 M'는 n개의 행과 $\frac{m_k\times{}_nC_p\times{}_{n-p}C_q\times\cdots\times{}_sC_s}{R!(k-R)!}$ 개의 열을 갖게 된다. M'에 의한 확장 화소의 수

$$m_1=\frac{m_k\times{}_nC_p\times{}_{n-p}C_q\times\cdots\times{}_sC_s}{R!(k-R)!} \tag{1}$$
$$(\text{or}\quad m_1=\frac{2^{k-1}\times\frac{n!}{p!\times q!\times\cdots\times s!}}{R!(k-R)!})$$

와 같이 되고, M'행렬에 대하여 백 화소를 위한 S_0'와 흑 화소를 위한 S_1'의 $n\times m_1$ 기저 행렬을 구할 수 있다.

3.2 휘도 분석

3.1절에 의해 구성된 (k, n)-VCS의 휘도를 분석하기 위해 임의의 k장의 슬라이드를 선택하는 경우를 고려한다. 각 행렬 S_0'와 S_1'에 대응하는 행들 가운데 $(r_1, r_2, \cdots, r_k)$의 조합이 한번 포함될 때마다 1만큼의 상대적 차가 반드시 생긴다. 따라서 휘도를 계산하기 위해서 n개 중 k개를 선택할 수 있는 모든 종류가 ${}_nC_k$이므로 전체 확장 화소의 수는 $2^{k-1}\times{}_nC_k$(단, $n=p+q+\cdots+s$)이고, 그 중에서 $(r_1, r_2, \cdots, r_k)$행을 반드시 한번씩 포함하는 경우의 수가 $p\times q\times\cdots\times s$회 나타나므로 상대 휘도는 다음과 같이 구할 수 있다.

$$\alpha=\frac{p\times q\times\cdots\times s}{2^{k-1}\times{}_nC_k} \tag{2}$$

또한, 행을 중복시킬 때 해밍 가중치가 같은 열이 생기게 되며, 이 열들을 제거하면 확장 화소의 수를 더욱 줄일 수 있다. 확장 화소의 수 m_1은 m을 $R!\times(k-R)!$로 나누는 만큼 줄어들므로 식(1)과 같이 구할 수 있고, 이 때 두 행렬 S_0'와 S_1' 각각에 대응하는 k개의 행들에 대하여 발생 가능한 "or" 해밍 가중치의 차 d를 산출하면

$$d=\frac{k!\times(n-k)!\times\frac{1}{R!(k-R)!}}{(p-1)!(q-1)!\cdots(s-1)!} \tag{3}$$

이 된다. 따라서, 상대 휘도 $\alpha=d/m_1$는

$$\alpha=\frac{p\times q\times\cdots\times s}{2^{k-1}\times{}_nC_k}$$

으로 되어 식(2)와 같음을 알 수 있다. 한편, $n \le pk$ 이므로

$$\alpha = \frac{p \times q \times \cdots \times s}{2^{k-1} \times {}_nC_k} > \frac{(k-1)!}{(2k)^{k-1}} \qquad (4)$$

이 성립된다. 즉, α는 n이 커져 m의 값이 증가하더라도 k에 의존하게 되므로 휘도가 향상된 (k, n)-VCS를 구성할 수 있다.

[예제1] (3,7)-VCS의 구성

먼저 (3,3)-VCS를 위한 S_0와 S_1을 구하면

$$S_0 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad S_1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

이고, 이 때 각 행의 인덱스는 다음과 같다.

$$r_1(S_0) = (0,1,1,0), \quad r_1(S_1) = (1,0,0,1)$$

$$r_2(S_0) = (0,1,0,1) = r_2(S_1)$$

$$r_3(S_0) = (0,0,1,1) = r_3(S_1)$$

n=7이므로 중복을 위한 열 벡터는 $V = [r_1, r_1, r_1, r_2, r_2, r_3, r_3]^T$이고, V에 대한 모든 행 교환 후의 연접행렬 M을 구하면

$$M = \begin{pmatrix} r_1 & r_1 & r_1 & r_1 & r_1 & r_1 & r_1 & r_1 & r_1 & \cdots & r_3 \\ r_1 & r_1 & r_1 & r_1 & r_1 & r_1 & r_1 & r_1 & r_1 & \cdots & r_3 \\ r_1 & r_1 & r_1 & r_1 & r_1 & r_1 & r_2 & r_2 & r_2 & \cdots & r_2 \\ r_2 & r_2 & r_2 & r_3 & r_3 & r_3 & r_1 & r_1 & r_1 & \cdots & r_2 \\ r_2 & r_3 & r_3 & r_2 & r_2 & r_3 & r_2 & r_3 & r_3 & \cdots & r_1 \\ r_3 & r_2 & r_3 & r_2 & r_3 & r_2 & r_3 & r_2 & r_3 & \cdots & r_1 \\ r_3 & r_3 & r_2 & r_3 & r_2 & r_2 & r_3 & r_3 & r_2 & \cdots & r_1 \end{pmatrix}$$

을 얻게 된다. 여기서 r_2와 r_3는 중복 횟수가 같으므로 열 교환에 의한 동일 열을 제거한 연접행렬 M'는 다음과 같다.

$$M' = \begin{pmatrix} r_1 & r_1 & r_1 & r_1 & r_1 & r_1 & \cdots & r_2 \\ r_1 & r_1 & r_1 & r_1 & r_1 & r_1 & \cdots & r_2 \\ r_1 & r_1 & r_1 & r_2 & r_2 & r_2 & \cdots & r_3 \\ r_2 & r_2 & r_2 & r_1 & r_1 & r_1 & \cdots & r_3 \\ r_2 & r_3 & r_3 & r_2 & r_3 & r_3 & \cdots & r_1 \\ r_3 & r_2 & r_3 & r_3 & r_2 & r_3 & \cdots & r_1 \\ r_3 & r_3 & r_2 & r_3 & r_3 & r_2 & \cdots & r_1 \end{pmatrix}$$

M'에 의해 (3,7)-VCS의 백 화소를 위한 기저행렬 S_0'와 흑 화소를 위한 기저행렬 S_1'을 각각 구할 수 있으며, 식(1)과 식(2)에 의해 확장 화소의 크기 m_1=420, 상대휘도 α=3/35이 된다.

3.3 (k, n)-VCS의 특수한 경우

3.1절에서 S_0와 S_1을 열 벡터 V에 따라 중복시킨 행렬들을 각각 S_0^*와 S_1^*라 하자. 이 S_0^*와 S_1^* 의 임의의 열에서 해밍 가중치가 같은 열을 제거하여 행 교환에 의한 연접행렬 S_0'와 S_1'을 새로이 구성한다. 이렇게 구성된 기저 행렬에 의해 확장 화소의 수와 상대 휘도를 더욱 개선시킬 수 있다. 각 행렬에서 제거된 열의 수를 e라고 할 때 상대 휘도 α는 식(5)와 같이 좋아지게 된다.

$$\alpha = \frac{p \times q \times \cdots \times s}{(2^{k-1} - e) \times {}_nC_k} \qquad (5)$$

[예제2] (3,4)-VCS의 구성

먼저, (3,3)-VCS의 S_0와 S_1의 첫 번째 열을 중복시켜 S_0^*와 S_1^*를 다음과 같이 구한다.

$$S_0^* = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad S_1^* = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

여기서 S_0^*의 4열과 S_1^*의 1열의 해밍 가중치는 각각 2가 되므로 이 두 열을 제거한 행렬 $S_0^{*\prime}$, $S_1^{*\prime}$는 다음과 같게 된다. 이 때 제거된 열의 수 e는 1이다.

$$S_0^{*\prime} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad S_1^{*\prime} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

여기서, 열 벡터 $V = [r_1, r_1, r_2, r_3]^T$이므로

$$M = \begin{pmatrix} r_1 r_1 r_1 r_1 r_1 r_1 r_2 r_2 r_2 r_3 r_3 r_3 \\ r_1 r_1 r_2 r_2 r_3 r_3 r_1 r_1 r_3 r_1 r_1 r_2 \\ r_2 r_3 r_1 r_3 r_1 r_2 r_1 r_3 r_1 r_1 r_2 r_1 \\ r_3 r_2 r_3 r_1 r_2 r_1 r_3 r_1 r_1 r_2 r_1 r_1 \end{pmatrix}$$

을 구성한 후, 중복횟수가 같은 경우를 고려한

$$\text{행렬 } M' = \begin{pmatrix} r_1 r_1 r_1 r_2 r_2 r_2 \\ r_1 r_2 r_2 r_1 r_1 r_3 \\ r_2 r_1 r_3 r_1 r_3 r_1 \\ r_3 r_3 r_1 r_3 r_1 r_1 \end{pmatrix}$$

에 의해서 기저 행렬 S_0'와 S_1'을 구하면 다음과 같게 된다. 이때 행렬 M 의 (1,2), (3,5), (4,6), (7,10), (8,11), (9,12)열의 쌍들은 열 교환의 결과가 같기 때문에 1개씩 삭제된 M'를 구할 수 있다.

따라서, 상대 휘도 α는 식(5)에 의해 1/6이 되어

$$S_0' = \begin{pmatrix} 0&1&1&0&1&1&0&1&1&0&1&0&0&1&0&0&1&0 \\ 0&1&1&0&1&0&0&1&0&0&1&1&0&1&1&0&0&1 \\ 0&1&0&0&1&1&0&0&1&0&1&1&0&0&1&0&1&1 \\ 0&0&1&0&0&1&0&1&1&0&0&1&0&1&1&0&1&1 \end{pmatrix},$$

$$S_1' = \begin{pmatrix} 0&0&1&0&0&1&0&0&1&1&0&1&1&0&1&1&0&1 \\ 0&0&1&1&0&1&1&0&1&0&0&1&0&0&1&0&1&1 \\ 1&0&1&0&0&1&0&1&1&0&0&1&0&1&1&0&0&1 \\ 0&1&1&0&1&1&0&0&1&0&1&1&0&0&1&0&0&1 \end{pmatrix}$$

식(2)에 의한 1/8보다 휘도가 개선됨을 알 수 있다. 즉, 동일한 해밍 가중치를 갖는 열을 제거함으로써 휘도를 개선시킬 수 있다. 특수한 (k, n)-VCS의 e값의 일부를 표 1에 제시하였다.

표 1. e의 크기

k\n	2	3	4	5	6	7	8
2							
3			1				
4				2	2		
5					6	6	5
6						12	14
7							29

제안방식에 의해 도출된 (k, n)-VCS의 확장 화소의 수 m_1과 상대 휘도 α의 일부를 표 2와 표 3에 각각 제시한다.

표 2. e값을 고려한 확장 화소의 수 m_1에 대한 비교

k\n	2	3	4	5	6	7	8	9
2	2	6	6	20	20	70	70	252
3		4	24 **(18)**	60	60	420	1,120	1,120
4			8	80 **(60)**	360 **(270)**	840	840	10,080
5				16	240 **(150)**	1,680 **(1,050)**	6,720 **(4,620)**	15,120
6					32	672 **(420)**	6,720 **(3,780)**	40,320
7						64	1,792 **(980)**	24,192

단, **(x)**는 e만큼의 열 제거에 의해 개선된 확장 화소의 수를 나타냄

3.4 확장화소의 크기를 줄이기 위한 새로운 구성

제안기법을 이용하면 n의 크기가 $2k$ 이상으로 커질 때 Droste 구성법[3]에 비해 휘도는 상당히 개선할 수 있으나, m_1의 크기가 너무 커져 현실적으로 구현이 곤란하게 된다. 따라서 3.3절에서 제안한 방법과 같은 휘도를 유지하면서 m_1의 크기를 줄일 수 있는 (k, n)-VCS의 새로운 구성법을 제안한다.

표 3. Droste기법과 제안기법의 상대 휘도 비교

k\n	방식	2	3	4	5	6	7	8	9
2	SD	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{1}{6}$	$\frac{1}{7}$	$\frac{1}{8}$	$\frac{1}{9}$
	3.1절	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{3}{10}$	$\frac{3}{10}$	$\frac{2}{7}$	$\frac{2}{7}$	$\frac{5}{18}$
	3.3절	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{3}{10}$	$\frac{3}{10}$	$\frac{2}{7}$	$\frac{2}{7}$	$\frac{5}{18}$
3	SD		$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{8}$	$\frac{1}{10}$	$\frac{1}{12}$	$\frac{1}{14}$	$\frac{1}{16}$
	3.1절		$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{10}$	$\frac{1}{10}$	$\frac{3}{35}$	$\frac{9}{112}$	$\frac{9}{112}$
	3.3절		$\frac{1}{4}$	$\mathbf{\frac{1}{6}}$	$\mathbf{\frac{1}{10}}$	$\frac{1}{10}$	$\frac{3}{35}$	$\frac{9}{112}$	$\frac{9}{112}$
4	SD			$\frac{1}{8}$	$\frac{1}{15}$	$\frac{1}{24}$	$\frac{1}{35}$	$\frac{1}{48}$	$\frac{1}{63}$
	3.1절			$\frac{1}{8}$	$\frac{1}{20}$	$\frac{1}{30}$	$\frac{1}{35}$	$\frac{1}{35}$	$\frac{1}{42}$
	3.3절			$\frac{1}{8}$	$\mathbf{\frac{1}{15}}$	$\mathbf{\frac{2}{45}}$	$\frac{1}{35}$	$\frac{1}{35}$	$\frac{1}{42}$
5	SD				$\frac{1}{16}$	$\frac{1}{30}$	$\frac{1}{48}$	$\frac{1}{70}$	$\frac{1}{96}$
	3.1절				$\frac{1}{16}$	$\frac{1}{48}$	$\frac{1}{84}$	$\frac{1}{112}$	$\frac{1}{126}$
	3.3절				$\frac{1}{16}$	$\mathbf{\frac{1}{30}}$	$\mathbf{\frac{2}{105}}$	$\frac{1}{77}$	$\frac{1}{126}$

※ SD는 S. Droste기법[3], 음영은 휘도가 개선되지 않은 부분, 볼드체는 e를 고려한 부분.

(k, k)-VCS의 S_0, S_1의 행을 $r_1, r_2, \cdots, r_k$로 구분하여 n개의 행으로 만들기 위해 중복시키면 해밍 가중치가 같은 열이 존재하게 된다. 이 열들을 제거한 후, 각각의 열들에 대한 모든 조합을 비율에 맞게 중복하여 나열하면 아래의 알고리즘에 의해 m_1의 크기를 줄일 수 있다.

[알고리즘 I] (k, n)-VCS의 구성

(1) (k, k)-VCS에 대한 기저행렬 S_0, S_1을 구성한다.

(2) S_0, S_1의 각 행 $r_1, r_2, \cdots, r_k$로부터 n행으로 확장하기 위한 열 벡터 V를 구한다.

(3) S_0, S_1의 각 행을 V에 따라 중복시켜 S_0^*, S_1^*를 구한 후, 각 열을 비교하여 해밍 가중치가 같은 열들을 제거한 행렬 $S_0^{*\prime}$, $S_1^{*\prime}$을 구한다.

(4) $S_0^{*\prime}$, $S_1^{*\prime}$의 각 열에서 해밍 가중치가 같은 열의 모든 조합을 찾아 나열하되, $S_0^{*\prime}$, $S_1^{*\prime}$의 각 열에서 해밍 가중치에 따른 열의 수에 대한 비율이 유지되도록 S_0'와 S_1'를 재구성한다.

[예제3] (3,4)-VCS의 새로운 구성

예제2에 의해 구성된 $S_0^{*\prime}$의 각 열에는 해밍 가중

치가 0인 열이 1개, 3인 열이 2개 존재한다. 따라서 행 교환에 의해 생길 수 있는 열의 종류는 각각 ${}_4C_0$ =1, ${}_4C_3$ =4,가 된다. $S_0^*{}'$에서 열의 해밍 가중치의 비율이 같도록 유지하려면 $2 \cdot {}_4C_0 : 1 \cdot {}_4C_3 = 1:2$로 되어 $m_1 = 2 \cdot {}_4C_0 + 1 \cdot {}_4C_3 = 6$이 된다. 같은 방법으로 $S_1^*{}'$의 각 열에서도 $m_1 = 6$이 되어 백 화소와 흑 화소를 위한 S_0'와 S_1'는 아래와 같이 구성된다.

$$S_0' = \begin{pmatrix} 1&1&1&0&0&0 \\ 1&1&0&1&0&0 \\ 1&0&1&1&0&0 \\ 0&1&1&1&0&0 \end{pmatrix}, \quad S_1' = \begin{pmatrix} 1&1&1&0&0&0 \\ 1&1&0&1&0&0 \\ 1&1&0&0&1&0 \\ 1&1&0&0&0&1 \end{pmatrix}$$

또한, 상대 휘도 α는 1/6로 예제2의 결과와 같으며, 이 구성법을 적용하면 표 4와 같이 3.3절에서 제안한 방법에 비해 확장 화소의 수 m_1이 줄게 됨을 알 수 있다.

표 4. 제안기법에 의한 확장 화소의 수(m_1)

k\n	방식	2	3	4	5	6	7	8	9
2	3.3절	2	6	6	20	20	70	70	252
	3.4절	2	6	6	20	20	70	70	252
3	3.3절		4	18	60	60	420	1,120	1,120
	3.4절		4	**6**	**20**	**20**	420	**112**	**112**
4	3.3절			8	60	270	840	840	10,080
	3.4절			8	**30**	**90**	**280**	**280**	**672**
5	3.3절				16	150	1,050	4,620	15,120
	3.4절				16	**30**	**210**	**308**	**1,008**

4. 복수의 휘도를 허용하는 새로운 구성법

3장에서 제안한 구성법들은 n의 크기가 커짐에 따라 휘도는 상당히 개선될 수 있으나, 확장 화소의 수 m이 크기 때문에 현실적으로 구현이 곤란한 문제가 여전히 남아 있다. 이 장에서는 복수의 휘도를 허용함으로써 m의 크기를 더욱 줄일 수 있는 (k, n)-VCS의 또 다른 구성법을 제안한다.

앞에서와 같은 방법으로 (k, k)-VCS에 대한 기저행렬 S_0, S_1의 각 행을 $r_1, r_2, \cdots, r_k$로 인덱싱 한다. (k, n)-VCS에 대한 기저 행렬을 구성하여 임의의 k 행으로 비밀 영상을 복원할 때 $\{r_1, r_2, \cdots, r_k\}$의 쌍이 적어도 한번 포함되어야만 최소한 1의 휘도 차가 발생함에 착안하여 확장 화소의 크기를 더욱 줄이는 구성법을 고안한다.

[알고리즘II] 복수휘도를 갖는 (k,n)-VCS구성

(1) (k, k)-VCS에 대한 기저행렬 S_0와 S_1을 구성한다.
(2) S_0와 S_1의 각 행을 $r_1, r_2, \cdots, r_k$로 인덱싱 한다.
(3) 모든 행을 각각 $p, q, \cdots, s$개씩 중복시켜 n ($n = p+q+\cdots+s$)개의 행을 구성하기 위한 열 벡터 V를 구한다.
(4) 3.1절과 같은 방법으로 V에 대한 모든 행을 교환하여 연접한 행렬에서 중복 부분을 제거한 행렬 M_1을 구성한다.
(5) M_1의 각 열에서 $\{r_1, r_2, \cdots, r_k\}$가 모두 포함된 조합을 찾아 나열한다.
(6) 제1열부터 마지막 열까지 비교하여 행에 대한 중복이 가장 적게 된 것부터 연결시켜 $r_1, r_2, \cdots, r_k$를 모두 포함하는 각 열의 조합을 연접한 행렬 M_2를 구한다.
(7) 연접된 열 내에 이미 포함된 열들은 모두 제거하면서 생성되는 행렬 M_2로부터 백 화소에 대한 기저 행렬 S_{02}와 흑 화소에 대한 기저 행렬 S_{12}를 얻는다.

[예제4] (2,4)-VCS의 구성

(1) 먼저 S_0와 S_1를 구한다.

$$S_0 = \begin{pmatrix} 0&1 \\ 0&1 \end{pmatrix}, \quad S_1 = \begin{pmatrix} 1&0 \\ 0&1 \end{pmatrix}$$

(2) 각 행을 위로부터 각각 r_1, r_2로 인덱싱 한다. 즉,

$$r_1(S_0) = (0,1), \quad r_1(S_1) = (1,0)$$
$$r_2(S_0) = (0,1) = r_2(S_1).$$

(3) n=4이므로 r_1, r_2를 중복시켜 M_1을 다음과 같이 구성할 수 있다.(p=2, q=2)

$$M_1 = \begin{pmatrix} r_1&r_1&r_2 \\ r_1&r_2&r_1 \\ r_2&r_1&r_1 \\ r_2&r_2&r_2 \end{pmatrix}$$

열의 수 $\frac{4!}{2! \times 2!} \times \frac{1}{2} = 3$인 행렬

(4) M_1의 각 열에서 $\{r_1, r_2\}$가 모두 포함된 조합을 찾아 나열한다.

제1열 $c_1 = \{(1,3), (1,4), (2,3), (2,4)\}$, $|c_1| = 4$
제2열 $c_2 = \{(1,2), (1,4), (2,3), (3,4)\}$, $|c_2| = 4$
제3열 $c_3 = \{(1,3), (1,4), (2,3), (2,4)\}$, $|c_3| = 4$

(5) 제1열부터 마지막 열까지 비교하여 $\{r_1, r_2\}$의 모든 조합이 적어도 한 번 이상 포함되면서 그

중복횟수가 최소가 되는 열들을 누적 연결하여 새로운 행렬 M_2를 구성한다. 여기서는 c_1과 c_2, c_1과 c_3, c_2와 c_3를 차례로 비교하면 $|c_1 \cup c_2| = |c_1 \cup c_3| = |c_2 \cup c_3| = 6$이므로 c_1에 c_2, c_3의 어느 것을 연접하여도 누적되는 조합의 수는 동일하게 된다. 여기서는 c_2를 연결시키면 $c_1 \cup c_2 \supset c_3$이므로 c_3를 제거하여 다음의 M_2를 구할 수 있다.

$$M_2 = \begin{pmatrix} r_1 \, r_1 \\ r_1 \, r_2 \\ r_2 \, r_1 \\ r_2 \, r_2 \end{pmatrix}$$

(6) M_2로부터 백 화소에 대한 기저 행렬 S_{02}와 흑 화소에 대한 기저 행렬 S_{12}를 구한다.

$$S_{02} = \begin{pmatrix} 1\ 0\ 1\ 0 \\ 1\ 0\ 1\ 0 \\ 1\ 0\ 1\ 0 \\ 1\ 0\ 1\ 0 \end{pmatrix}, \quad S_{12} = \begin{pmatrix} 1\ 0\ 1\ 0 \\ 1\ 0\ 0\ 1 \\ 0\ 1\ 1\ 0 \\ 0\ 1\ 0\ 1 \end{pmatrix}$$

이 때, 확장 화소 수 $m_2=2\times2=4$, 상대 휘도의 평균은 $\tilde{\alpha} = (\frac{1}{2}\times2+\frac{1}{4}\times4)/6=\frac{1}{3}$인 복수의 휘도가 나타난다. 또한, 예제4와 같은 방법으로 (3,7)-VCS를 위한 연접행렬 M_2와 기저행렬 S_{02}, S_{12}는 아래와 같이 얻어진다.

$$M_2 = \begin{pmatrix} r_1\ r_1\ r_1\ r_1\ r_1 \\ r_1\ r_2\ r_2\ r_3\ r_1 \\ r_1\ r_3\ r_2\ r_1\ r_2 \\ r_2\ r_1\ r_3\ r_1\ r_2 \\ r_2\ r_2\ r_1\ r_2\ r_3 \\ r_3\ r_3\ r_1\ r_2\ r_3 \\ r_3\ r_1\ r_3\ r_3\ r_1 \end{pmatrix},$$

$$S_{02} = \begin{pmatrix} 01100110011001100110 \\ 01100101010100110110 \\ 01100011010101100101 \\ 01010110001101100101 \\ 01010101011001010011 \\ 00110011011001010011 \\ 00110110001100110110 \end{pmatrix},$$

$$S_{12} = \begin{pmatrix} 10011001100110011001 \\ 10010101010100111001 \\ 10010011010110010101 \\ 01011001001110010101 \\ 01010101100101010011 \\ 00110011100101010011 \\ 00111001001100111001 \end{pmatrix}$$

그림2는 S_{02}와 S_{12}으로부터 구현된(3,7)-VCS을 나타낸다. (a)는 분산시키기 위한 원 영상이며, (b)~(h)는 각 share가 랜덤함을 알 수 있다. 여기서 (3,3)-VCS에 대한 확장 화소의 수가 m=4이므로 (3,7)-VCS에서의 확장 화소의 수 $m_2=4\times5=20$이 되고, 상대 휘도의 평균은 $\tilde{\alpha}=3/35$이 된다.

그림 3에 share들의 조합에 따라 비밀정보가 나타남을 보여주고 있다. (3,7)-VCS에서는 (α)와 같이 2장 이하의 슬라이드를 겹치면 비밀정보가 복원되지 않지만, 3장의 슬라이드를 겹치면 비밀이 복원되며, 겹치는 슬라이드의 조합에 따라 복수의 휘도를 얻을 수 있는 특징을 갖게 된다. 또한, {2, 4, 6}행의 중첩일 때는 {1, 2, 3, 4, 5, 6, 7}의 모든 행을 겹친 경우와 동일한 휘도를 얻을 수 있다.

그림4에서는 (3,7)-VCS에서 S_{02}와 S_{12}를 M_4와 같이 4회 중복시켜 확장하였을 때 휘도가 어떻게 변화하는지 살펴보았다. 그 결과, m_4=80으로 증가시키면 시각적으로 약간 선명하게 느껴지나, 이는 복원 영상의 크기 변화에 따른 효과이지 휘도 자체가 개선된 것은 아니다. 한편, 휘도에 대하여 시각적 효과를 고려한 새로운 정의를 위한 연구가 시도되고 있다[7].

$$M_4 = \begin{Bmatrix} r_1r_1r_1r_1r_1 & r_1r_1r_1r_1r_1 & r_1r_1r_1r_1r_1 & r_1r_1r_1r_1r_1 \\ r_1r_2r_2r_3r_1 & r_1r_2r_2r_3r_1 & r_1r_2r_2r_3r_1 & r_1r_2r_2r_3r_1 \\ r_1r_3r_2r_1r_2 & r_1r_3r_2r_1r_2 & r_1r_3r_2r_1r_2 & r_1r_3r_2r_1r_2 \\ r_2r_1r_3r_1r_2 & r_2r_1r_3r_1r_2 & r_2r_1r_3r_1r_2 & r_2r_1r_3r_1r_2 \\ r_2r_2r_1r_2r_3 & r_2r_2r_1r_2r_3 & r_2r_2r_1r_2r_3 & r_2r_2r_1r_2r_3 \\ r_3r_3r_1r_2r_3 & r_3r_3r_1r_2r_3 & r_3r_3r_1r_2r_3 & r_3r_3r_1r_2r_3 \\ r_3r_1r_3r_3r_1 & r_3r_1r_3r_3r_1 & r_3r_1r_3r_3r_1 & r_3r_1r_3r_3r_1 \end{Bmatrix}$$

5. 결 론

시각암호의 휘도를 개선하기 위하여 (2, n)- VCS에 대한 여러 가지 기법이 연구되어 왔으며[6], (k, n)-VCS에 대해서는 S. Droste에 의해 m을 줄임으로서 휘도를 개선하기 위한 연구가 있었다[3]. Droste 방법이 확장 화소의 크기를 줄이는데 중점을 둔 것에 비하여, 본 논문에서는 확장 화소의 값에 큰 영향을 받지 않고 휘도를 개선하는데 중점을 두고 있다. 그 결과, n이 $2k$ 이하의 경우는 m이 커져도 중복이 되지 않는 관계로 휘도가 크게 개선되지 못하였지만, 특수한 일부의 경우 개선되었고, n이 $2k$이상일 경우는 모든 열에 대한 중복도가 최소한 1이상이 되므로 휘도가 상당히 개선되었다. 같은 휘도일 경우에 m의 크기가 커지더라도 비밀을 복원하는데는 차이가 없으므로 n이 커져서 휘도를 개선해야 할 경우나 복수의 휘도를 허용하는 경우에 매우 개선된 휘도를 얻을 수 있었다. 향후의 과제로 복수의 휘도를 허용할 경우에 있어서의 규칙적인 행렬 구성법의 연구가 남아 있다.

(a) 원영상

(b) share1

(c) share2

(d) share3

(e) share4

(f) share5

(g) share6

(h) share7

그림 2. (3,7)-VCS 분산 Shares(m=20)

(a) share1 ∪ share2

(b) share2 ∪ share4 ∪ share5

(c) share2 ∪ share4 ∪ share6 or All shares

(d) share1 ∪ share2 ∪ share3 ∪ share4 ∪ share5

그림 3. (3,7)-VCS의 복원영상(m=20)

(a) share1 ∪ share2

(b) share2 ∪ share4 ∪ share5

(c) share2 ∪ share4 ∪ share6 or **All shares**

(d) share1 ∪ share2 ∪ share3 ∪ share4 ∪ share5

그림 4. (3,7)-VCS 복원영상(m=80)

참 고 문 헌

[1] A. Shamir, "How to Share a Secret", Communications of the ACM, Vol.22, no.11, pp.612- 613, Nov. 1979.
[2] M. Naor and A. Shamir, "Visual cryptography", Proc. of Eurocrypt'94, Springer-Verlag, pp.1-12, Apr. 1994.
[3] S. Droste, "New Results on Visual Cryptography", Proc. of Crypto'96, Springer-Verlag, pp.401-415, Aug. 1996.
[4] E. R. Verheul, H. C. A. Tilborg, "Constructions and Properties of k out of n Visual Secret Sharing Schemes", Designs, Codes, and Cryptography, 11, pp.179-196, 1997
[5] 최창근, 박지환, "시각암호에서 계층적 접근구조에 따른 휘도 분석과 개인식별에 응용, 한국통신정보보호학회 논문지 8권 2호, pp.13-26 1998. 6
[6] C. Blundo, A. De Santis and D. R. Stinson, "On the Contrast in Visual Cryptography Schemes", J.of Cryptology, 12, pp.261-289, 1999
[7] P. A. Eisen, D. R. Stinson, "Threshold Visual Cryptography Schemes with Specified Whiteness Levels of Reconstructed Pixels", submitted to Designs, Codes, and Cryptography, Oct. 1999

양 신 석

1984년 2월 동아대학교 수학과 졸업
1997년 8월 부경대학교 전산정보학과 석사
1996년 3월 ~ 현재 배정고등학교 교사
관심분야 : 정보보호 및 정보이론

김 문 수

1982년 2월 부산대학교 수학교육과 졸업
1997년 8월 부산대학교 수학교육과 석사
2000년 8월 부경대학교 전자계산학과 박사과정 수료
2000년 3월 ~ 현재 부산여자고등학교 교사
관심분야 : 정보보호 및 암호학

박 지 환

1990년 3월 일본 요코하마국립대학 전자정보공학 졸업(공학박사)
1994년 9월 ~ 1995년 3월 동경대학 생산기술연구소 방문연구
1998년 1월 ~ 1998년 2월 일본 전기통신대학, 방문연구
1999년 7월 ~ 1999년 8월 Monash University, Australia, Visiting Research
2001년 2월 ~ 2001년 3월 Communication Research Laboratory, Japan, STA Fellowship
1996년 4월 ~ 현재 동경대학 생산기술연구소 협력연구원
1990년 3월 ~ 현재 부경대학교 전자컴퓨터정보통신공학부 교수
1997년 3월 ~ 현재 한국통신학회 부호 및 정보이론 연구회 운영위원
1997년 3월 ~ 현재 한국통신정보보호학회 이사 및 영남지부 부지부장
1998년 12월 ~ 현재 한국멀티미디어학회 총무이사
1999년 3월 ~ 현재 한국정보처리학회 논문지 편집위원
관심분야 : 멀티미디어 압축 및 응용, 정보보호 및 암호학